

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF:
The premises known as the offices of
Dropbox, Inc., located at 333 Brannan
St., San Francisco, CA, 94107, for the
account associated with Trevor Hylle
and trevorhylle97@gmail.com

CR

19-MJ-35

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION**

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

1. I, Brian Freeouf, Investigator with the Pennington County Sheriff's Office (PCSO) and currently assigned to the South Dakota Internet Crimes Against Children Taskforce (ICAC), being duly sworn, states as follows:

2. I began my law enforcement career with Pennington County in July of 2005. I spent approximately 3 years on patrol in the contract community of Wall, SD. I was then assigned to the patrol division in Rapid City in 2008. I was promoted to the rank of Senior Deputy in July of 2010. I also spent time as a School Liaison Officer and Criminal Investigations Division as a Property Crimes Investigator. Even though I was assigned as a Property Crimes Investigator I also investigated other crimes including, but not limited to, homicides, rapes, assaults, and coroner duties. My other assignments within the Sheriff's Office include Deputy Coroner, Field Training Deputy, and Defensive Tactics Training Administrator. Due to the placement on ICAC, I have also been given the title of Special Assistant Attorney General of the State of South Dakota.

3. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statutes 18 U.S.C. §§ 2251, 2252 and 2252A. During my law enforcement-career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography and those who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

4. I have been informed that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the manufacture, distribution, receipt and possession of child pornography.

5. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals, including other law enforcement officers, interviews of persons with knowledge, my review of documents, interview reports and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, I have not withheld information known to me that would tend to negate probable cause has

been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

6. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a drop box account found during the investigation of an unknown Dropbox user, which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography). The items are more specifically described in Attachment B. The Dropbox, Inc. account is associated with email: Trevorhülle97@gmail.com (also referred to in this affidavit as “Target Account”) from the date the user opened the Dropbox Inc. account to the date of this search warrant.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments A and B:

a. “Chat,” as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Chat room”, as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in

real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. “Cloud-based storage service,” as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file.

Access is free and readily available to anyone who has an internet connection.

f. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

g. “Computer hardware,” as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. “Computer software,” as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

l. “Electronic Storage Device” includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with

storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

m. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

o. “Hyper Text Markup Language”, or “HTML”, as used herein, is a standard protocol for formatting and displaying documents, such as web pages, on the Internet.

p. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

q. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including

access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

r. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

s. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

t. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

u. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

v. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

w. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send

short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

x. “Storage medium” A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

y. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, EMAIL AND FILE SHARING SERVICES

8. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. File sharing services, like Dropbox, Inc., are commonly utilized for both legitimate file sharing as well as illicit file sharing.

b. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit

children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

c. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email, like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

d. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People

can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “instant messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

f. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user’s computer or external media in most cases.

9. Based on my training and experience and investigation in this case, I have learned the following about Dropbox, Inc.:

- a. Dropbox is a file syncing and collaboration service that allows users to access and share their files on computers, phones, tablets and the Dropbox website.
- b. Each Dropbox account is associated with a single email address at any given point. If a user were to share login information for an account, more than one person could plausibly take actions in the Dropbox account at the same time, but would all appear as the same user to Dropbox.
- c. IP addresses of specific actions within a Dropbox account, such as uploads and deletions, are not available.
- d. IP address login information is recorded when a user logs in to Dropbox through Dropbox's website. Like many online services, Dropbox sometimes uses cookies stored on a browser so that a user may not need to sign in every time they visit the website. Additionally, if a user is accessing files in their Dropbox account from a desktop or mobile application, that access may not be logged by Dropbox.
- e. If a Dropbox user is a member of a shared folder, then other members of the shared folder can also upload content. Also, if a user shares their login information (email and password), then other people could login and upload files. Users can use the "file request"

feature to receive files directly on their Dropbox from another person, even if that person does not have a Dropbox account.

- f. “Dropbox” refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

- g. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone

numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

- h. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.
- i. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects

to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

- j. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

10. From my training and experience, I am aware that Dropbox's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

11. On 02/20/19, I received a CyberTipline Report from the National Center of Missing and Exploited Children (NCMEC). The report number is 45173013. The report was generated Dropbox. This was in reference to someone uploading and storing child pornography on a Dropbox account. This information was reported to NCMEC on 01/03/19 at 00:39:30 UTC.

12. I know that Dropbox is a file hosting service, cloud storage service, online file storage provider, or cyberlocker is an internet hosting service specifically designed to host user files. It allows users to upload files accessible over the internet after a user provides a user name and password or other authentication. The cybertip provided the following information reference the user of the reported account:

Email Address: Trevorhülle97@gmail.com

Screen/User Name: Trevor Hülle

ESP User ID: 473487220

13. Dropbox reported 36 uploaded files contained contraband. I viewed the files and 35 of the 36 are child pornography. The last file was a log file which contained the Dropbox activity. The following is a sample of the files reported in the cybertip:

- File Name: 0e0167d2-a643-4a2a-b7a8-2a1db80aadd9-2.jpg
 - Description: This image shows an approximately 8-10 year old boy being orally raped by an erect adult male penis.
- File Name: _ - Yamad Boy 13Yo - 14Yo - Russian Piss.avi
 - Description: This is a 24 minute and 49 second video. The video starts with two boys approximately 8-10 year old boys lying on a bed totally naked. The boys are kissing and one starts to perform oral sex on the other boy. At 5 minutes the boys have changed positions but one is still performing oral sex on the other boy. At 10 minutes one of the boys is having anal sex from behind with

the other boy. At 20 minutes one of the boys is on his back with his legs up in the air and the other boy is having anal sex with that boy. The video ends with one of the boys performing oral sex on the other boy.

- File Name: kdv-2 11yo boys take care of a 10yo friend.avi
 - Description: This is a 35 minute and 52 second video. The video starts with 3 boys approximately 8-10 years of age on a bed. They are all clothed at the beginning of the video. At 5 minutes one of the boys is completely naked and the other two are still clothed. One boy and kissing and sucking on the naked boy's nipples and the other is performing oral sex on the naked boy. At 15 minutes all three boys are naked. One is lying on his back with a second boy on top of him on his hands and knees. These two boys are performing oral sex on each other. The third boy is attempting to have anal sex with the boy on his hands and knees. At 30 minutes one boy is on his back with his legs over the shoulders of another boy who is on his knees. The boy on his knees is having anal sex with the boy on his back. The third boy is giving oral sex to the boy who is on his back receiving the anal sex. The video ends with all three boys still naked kneeling next to each other on the bed with their arms around each other.
 - There are two more video files with the rest of the reported files. The total length of all child pornography videos included in the

report is 69 minutes and 25 seconds.

- File Name: e9362251-9e4c-46a5-8245-ae520e2433a0-2.jpg
 - Description: An approximately 5-8 year old boy sitting on the lap of an adult male. The boy is completely naked exposing his bare penis. The adult has his pants unzipped and open. The boy has pulled the adult males penis out of his pants and has both hands holding it.
- File Name: d73d586f-68c5-44fc-818d-714dfd68fb8b-2.jpg
 - Description: This image has 3 boys all approximately 8-12 years of age. One boy is standing and has his shorts and underwear pulled down exposing his penis. A second boy is on his knees in front of the first boy. This boy is not wearing a shirt and has his shorts pulled down to his knees exposing his penis. This boy is performing oral sex on the boy who is standing. There is a third boy that is fully clothed and lying on his stomach between the legs of the standing boy. This boy is performing oral sex on the second boy that is kneeling.

14. Based on the information provided to me through the NCMEC report I created and served a subpoena on Google for any subscriber and user information of trevorhülle97@gmail.com. This was in an attempt to get a better location of where the suspect is located through IP address or phone numbers. Google responded with the following information:

Name: Diesality 2001

e-Mail: trevorhülle97@gmail.com

Services: Android, Gmail, Google Calendar, Google Chrome Sync, Google Cloud Print, Google Developers Console, Google Docs, Google Drive, Google Hangouts, Google My Maps, Google Payments, Google Photos, Google Play, Google Play Music, Google+, Has Google Profile, Has Plusone, Is In Family, Location History, Web & App Activity, YouTube

Recovery e-Mail: trevorhülle@yahoo.com

Created on: 2014/08/27-20:38:04-UTC

Terms of Service IP: 68.69.72.41, on 2014/08/27-20:38:04-UTC

SMS: +16055154415 [US]

Google Account ID: 273223983512

Last Logins:

- 2019/02/08-01:11:56-UTC, 2019/01/30-03:19:30-UTC
- 2019/02/08-01:11:56-UTC;
2600:1014:b02f:9501:dcc7:8078:f5ed:4eed | Login |
- 2019/02/08-01:11:56-UTC
2600:1014:b02f:9501:dcc7:8078:f5ed:4eed | Login |
- 2019/01/30-03:19:34-UTC | 174.219.9.214 | Login |
- 2019/01/30-03:19:30-UTC | 174.219.9.214 Login |
- 2019/01/24-02:21:03-UTC | 174.219.16.0 | Login |
- 2019/01/24-02:20:39-UTC |
2600:1014:b012:6a06:1d97:d8d:3459:86af | Login |
- 2019/01/24-02:20:29-UTC | 174.219.16.0 | Login |

- 2019/01/24-02:20:21-UTC | 174.219.16.0 | Login |
- | 2019/01/24-02:20:17-UTC | 174.219.16.0 | Login |
- 2019/01/24-02:20:15-UTC
2600:1014:b012:6a06:1d97:d8d:3459:86af | Login |
- 2019/01/21-22:31:45-UTC | 66.231.7.210 | Logout |
- 2019/01/21-22:14:43-UTC | 66.231.7.210 | Login
- 2019/01/21-19:25:57-UTC | 209.159.199.173 | Logout |
- 2019/01/21-19:24:10-UTC | 209.159.199.173 | Login |
- 2019/01/21-19:23:03-UTC | 209.159.199.173 | Logout |
- 2019/01/21-19:20:16-UTC | 209.159.199.173 | Login |
- 2019/01/19-22:32:03-UTC
2600:1014:b067:c8bc:1885:a19b:a85d:2250 | Login |
- 2019/01/19-22:32:02-UTC | 174.219.153.34 | Login

15. Eight consecutive Login events from IP 209.159.225.162 occurred during past 24 hours prior to the following event:

- 2019/01/08-02:02:43-UTC | 209.159.225.162 | Login |

16. The following is what I found during my investigation of the above listed IP addresses:

The following IP address are utilized by Verizon Wireless:

- 2600:1014:b02f:9501:dcc7:8078:f5ed:4eed
- 174.219.9.214
- 174.219.16.0
- 2600:1014:b012:6a06:1d97:d8d:3459:86af
- 2600:1014:b067:c8bc:1885:a19b:a85d:2250

- 174.219.153.34

The following IP address are utilized by Vast Broadband:

- 209.159.199.173
- 209.159.225.162

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL
INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS
CHILD PORNOGRAPHY**

17. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

- a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual

arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. The possessor typically keeps the child pornography close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or

meet others to share information and materials. These individuals rarely destroy correspondence from other child pornography distributors/possessors or conceal such correspondence as they do their sexually explicit material. They often maintain lists of names, addresses, and telephone numbers of individuals they have been in contact with who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time-period. Law enforcement officers involved in the investigation of child pornography throughout the world have documented this behavior. Thus, even if the unknown user uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not an examiner will find evidence of this access within the SUBJECT ACCOUNT.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

18. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

19. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a “district court of the United States (including a magistrate judge of such court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

20. The United States respectfully applies for an order of nondisclosure to Google, Inc. under 18 U.S.C. § 2705(b) regarding the Dropbox, Inc. account associated with email address Trevorhülle97@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Dropbox, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account

information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Dropbox, Inc., persons can modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Dropbox, Inc. not to notify the user of the existence of this warrant.

REQUEST FOR SEALING OF MATTER

21. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

LIMIT ON SCOPE OF SEARCH

22. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

23. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Dropbox, Inc., contain evidence of crimes, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the

electronic accounts described in Attachment A. The facts outlined above show that the Dropbox, Inc. account, listed in Attachment A have been used for the exploitation of children using the internet including violations of 18 U.S.C. §§ 2252, 2252A (production, receipt and possession of child pornography), which items are more specifically described in Attachment B. There is probable cause to believe that the unidentified user of the Dropbox, Inc. account received and distributed child pornography with other unknown users and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The account is the subject of this warrant affidavit. The accounts the Dropbox Inc. account associated with an unknown user and email Trevorhülle@gmail.com.

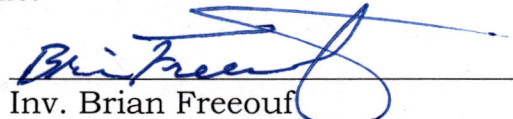
24. Law Enforcement agents will serve the warrant on Dropbox, Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

25. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, and for the Court to authorize search of the items seized in an off-site controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on Dropbox, Inc. via the

internet and to allow Dropbox, Inc. to copy the data outside of this agent's presence.

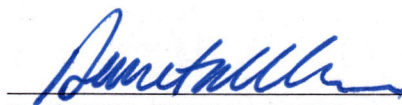
RETURN COMPLIANCE BY DROPBOX, INC.

26. Dropbox's policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant, instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Specifically, Dropbox requires the Court order the disclosure, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

 3/27/19
Inv. Brian Freeouf
Pennington County Sheriff's Office
and Internet Crimes Against
Children Taskforce

SUBSCRIBED and SWORN to in my presence

this 27 day of March, 2019.


DANETA WOLLMANN
U.S. MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with the following Dropbox, Inc. account known to be stored at the premises controlled by Dropbox, Inc., located at 333 Brannan St., San Francisco, CA, 94107. Account information: the Dropbox, Inc. account associated with an unknown user and email address Trevorhülle97@gmail.com.

ATTACHMENT B
**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

I. Information to be disclosed by Dropbox Inc. (the “Provider”) to facilitate execution of the warrant:

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox Inc., including any emails, records, files, logs, or information that have been deleted but are still available to Dropbox Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 18, 2019. Dropbox Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in the email account which is helpful to determine the accounts’ user’s or owner’s true identity:

a. All content of files associated with the account, from the time of the account’s creation to the present, including stored or preserved images, communications or other files.

b. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

c. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails “invites” sent or received via Dropbox, and any contact lists.

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files and information regarding shared accounts;

f. All records pertaining to communications between Dropbox Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after the creation of the account that is the subject of this warrant and that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, (production, receipt and possession of child pornography), including, for the account or identifiers listed on Attachment A, information pertaining to the following matters:

a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or attempting or conspiring to do so;

b. Any person knowingly distributing, receiving, or possessing child pornography as defined at 18 U.S.C. § 2256(8), or attempting or conspiring to do so;

c. Any person knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged, or attempting to do so;

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the email account owner or user;

e. Evidence indicating the email account users or owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

g. Records relating to who created, used, or communicated with the electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram.

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evidence of their whereabouts;

4. Evidence of the times the user utilized the account or identifiers listed on Attachment A;

5. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifier listed on Attachment A and other associated accounts.

III. Information Regarding Search Warrant Compliance by Google:

Dropbox Inc. shall disclose responsive data, if any, by sending to:

Inv. Brian Freeouf
Internet Crimes Against Children Taskforce
Freeouf@pennco.org
300 Kansas City Street, Suite 200
Rapid City, SD 57701
(605) 377-7420

Dropbox shall use the United States Postal Service or another courier service to disclose the responsive data, notwithstanding 18 U.S.C. § 2252A or similar statute or code. In the alternative, Dropbox may make the responsive data available to Investigator Freeouf by use of its law enforcement website.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL
RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Dropbox Inc., and my official title is

_____. I am a custodian of records for Dropbox Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Dropbox Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Dropbox Inc.; and

c. such records were made by Dropbox Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature